IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Patent Application

Appellants: Junbiao Zhang et al.

Examiner: Nathan A. Mitchell

Serial No: 10/550,964

Group Art Unit: 2617

Filed: September 26, 2005

Confirmation No.: 6118

For: SECURE ROAMING BETWEEN WIRELESS ACCESS POINTS

Mail Stop Appeal Brief-Patents
Hon. Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Pursuant to the Notice of Appeal filed June 9, 2009, Appellants submit this Appeal Brief to appeal the status of Claims 1, 4, and 5 as rejected in the Final Office Action dated January 22, 2009, and the Advisory Action dated April 28, 2009.

Appellants hereby request a one-month extension to provide for timely submission of this Appeal Brief. The Commissioner is authorized to charge the Appeal Brief fee and the extension fee (or other applicable fees) to **Deposit Account No. 07-0832**.

TABLE OF CONTENTS:

1. Real Party in Interest

The real party in interest is THOMSON LICENSING S.A.

2. Related Appeals and Interferences

None.

3. Status of Claims

Claims 1–19 are pending. Claims 1, 4, and 5 stand rejected and are under appeal. Claims 2 and 3 stand objected to as depending from a rejected base claim. Claims 6, 7, 9–11, and 13–19 have been allowed.

A copy of the Claims 1–19 is presented in Section 8 below.

4. Status of Amendments

A response under 37 C.F.R. § 1.116 was filed with the PTO on April 22, 2009. The response made no amendments, and no further amendments subsequent to the issuance of the Final Office Action on January 22, 2009 have been made or entered.

5. Summary of Claimed Subject Matter

Embodiments of the present invention are generally directed to a system, method, and computer readable medium for enabling roaming of wireless client stations among wireless access points. A gateway programmed to receive session data requests is provided in a network, which comprises access points that are programmed to send session data requests to the gateway. The gateway sends session information setting commands to the requesting access point, or sends a session data failure response to the access point. (See Abstract.)

Appellants' claims 1, 4 and 5 are presented below in claim format with elements reading on the various figures of the drawings (with reference numerals, where applicable) and appropriate citations to at least one portion of the specification (paragraph numbers refer to those in the published application US 2006/0193297 A1) for each element of the appealed claims.

Claim 1 recites:

1. A communications system, comprising:

a gateway *(15)* connected to a wired network *(14)*; (*e.g., paragraph 29 and FIG. 1)* and

a plurality of access points *(11-13)* associated with, and controlled by, the gateway, (*e.g., paragraphs 12, 29, and FIG. 1)*

wherein each access point is configured (i) to wirelessly communicate with and receive association requests from wireless clients for connection to the wired network through the access point (*e.g., paragraphs 30–33 and FIG. 4, step 20)* (ii) to send session information requests to the gateway in response to received association requests (*e.g., paragraphs 30–33 and FIG. 4, step 21)* and

(iii) to process session information setting commands received from the gateway, *(e.g., paragraphs 32-33 and FIG. 4)*

wherein the gateway is configured (i) to maintain session information that currently exists for each wireless client connected to the wired network through an access point associated with the gateway, the session information including a session key associated with each wireless client and an associated access point, *(e.g., paragraphs 30-33 and FIG. 4, step 22)* and (ii) to respond to a session information request from a given access point by providing that access point with currently existing session information, if any, maintained by the gateway for the wireless client requesting association with that access point. *(e.g., paragraphs 30–33 and FIG. 4, step 29)*

Claim 4 recites:

4. The system of claim 1 having means to ensure that a connection between the gateway and an access point is trusted. *(e.g., paragraph 21)*

Claim 5 recites:

5. The system of claim 4 wherein the means comprises physical security or encryption. *(e.g., paragraph 21)*

6. Grounds of Rejection to be Reviewed on Appeal

Claim 1 stands rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Publication No. 2004/0203771 to Chang et al. in view of U.S. Patent Publication No. 2008/0119184 to Rebo et al.

Claims 4 and 5 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Publication No. 2004/0203771 to Chang et al. in view of U.S. Patent Publication No. 2008/0119184 to Rebo et al. and further in view of U.S. Patent Publication No. 2002/0046179 to Kokudo.

7. Argument

A. Introduction

In general, the present invention is directed to a technique for secure roaming between wireless access points. As disclosed in the Appellants' specification in paragraphs 5–7 of the published application US2006/0193297:

> "The IEEE 802.1x standard addresses the security problem in IEEE 802.11 by using port controlled access control. In a large 802.1x installation, a backend authentication server authenticates the user. In order to secure the wireless link, the wireless station must go through an authentication process involving the station, the access point and the authentication server. If authentication is successful, a session key is agreed upon between the wireless station and the access point. This solution enables roaming, but with high overhead, i.e., each time a station is associated with a different access point, for example because of signal fluctuation, the whole authentication process has to be carried through. This is highly undesirable, especially when the authentication server is far away from the wireless LAN, e.g., in an inter-working environment where the WLAN is in, for example, JFK airport but the authentication server belongs to, for example, SBC in California.
>
> There is a need to provide seamless roaming when a wireless user (client) wishes to switch to an access point with better signal strength.
>
> There is also a need to move per-user session keys and authorization information from one access point to another when a client roams between wireless access points."

Advantageously, the present principles provide a communication system which addresses these problems.

The claims of the pending invention include novel features not shown in the cited references and that have already been pointed out to the Examiner. These features provide advantages over the prior art and dispense with prior art problems such as those described above with reference to the Applicant's specification.

It is respectfully asserted that independent Claim 1 is patentably distinct and non-obvious over the cited references in its own right. For example, the below-identified limitations of independent Claim 1 are not shown in any of the cited references, either taken singly or in any combination. As such, independent Claim 1 is patentable and presented for review in this appeal. It is further respectfully asserted that Claims 4 and 5 recite patentable subject matter above and beyond that recited in Claim 1 and are thus separately patentable and presented for review in this appeal.

B. Whether Claim 1 is Unpatentable Under 35 U.S.C. §103(a) Over U.S. Patent Publication No. 2004/0203771 to Chang et al. in view of U.S. Patent Publication No. 2008/0119184 to Rebo et al.

Claim 1 is rejected as being unpatentable over U.S. Patent Publication No. 2004/0203771 to Chang et al. (hereinafter "Chang") in view of U.S. Patent Publication No. 2008/0119184 to Rebo et al. (hereinafter "Rebo"). The Examiner contends that the cited combination shows all the limitations recited in Claim 1.

Chang is directed to a "method of managing information about mobile terminal in a mobile communication system supporting high-rate data transmission" (Chang, Title). In further detail, Chang discloses the following in the Abstract:

> "A method of managing the session information of an AT in a CDMA2000 IxEV-DO system. In the IxEV-DO system, a service system, having an SC/MM, is connected to a PDSN, a plurality of ANs are connected to the service system, and a plurality of ATs are capable of wireless communication with the ANs. In the session information managing method, an AN transmits to the SC/MM a session retrieve request message, upon receipt of a connection request message from the AT. The SC/MM then searches for session information of the AT and transmits to

> the AN a session retrieve response message including the session information. Upon receipt of the session retrieve response message, the AN transmits a connection response message to the AT."

Rebo is directed to a "method for fast, secure 802.11 re-association without additional authentication, accounting, and authorization infrastructure" (Rebo, Title). In further detail, Rebo discloses the following in the Abstract:

> "A method wherein an access point authenticates itself with neighboring access points and establishes secure and mutually authenticated communication channels with its neighboring access points. When an access point learns of a neighboring access point, it initiates an authentication with an authentication server through the neighboring access point. Once access points have mutually authenticated each other, whenever a station authenticates itself with a first access point, the first access point communicates the station's authentication context information, for example session key and session identifier, to each neighboring access point. Thus, when the station roams to a neighboring access point, the neighboring access point presents the station with a reauthentication protocol, for example LEAP reauthentication, and if the reauthentication is successful, communication between the station and the neighboring access point takes place immediately and no new EAP authentication needs to occur."

It will be shown below that the limitations of Claim 1 reproduced herein are not shown in the cited references, and that Claim 1 should be allowed.

B1. Claim 1

Initially, it is respectfully pointed out that Claim 1 recites, *inter alia*, "a gateway connected to a wired network." The Examiner asserts variously that this element is disclosed by Chang's elements 50, 100, and the combination thereof (e.g., Final Office Action, p.2; Advisory Action). However, it must be noted that Chang never discloses or suggests a gateway of any sort.

A "gateway" is a simple concept to those having ordinary skill in the art. For example, Webopedia (http://www.webopeia.com, an online encyclopedia dedicated to computer technology) defines "gateway as: (n.) (1) A node on a network that serves as an entrance to another network. Those skilled in the art would therefore recognize that a "gateway" functions to pass information between discrete networks. Local traffic, within a shared network, does not pass through the gateway, while traffic meant for the outside is sent along by the gateway. Chang defines its GAN 100 as a "General ATM switch Network." *See* Chang, ¶21. The plain meaning of a GAN is therefore a single network, and Chang does not modify or add to that definition to include other networks, or to include a device which might allow communication with other networks. Devices attached to such a GAN (such as Chang's data location register (DLR) 50 or packet data serving node (PDSN) 60) are able to communicate with one another without the use of a gateway. Chang's GAN 100 is analogous to a physical Ethernet, with cables and switches, connecting the various devices in a LAN. In no way is a gateway required by such a network, nor is any implied by Chang's usage.

Furthermore, the DLR 50 that the Examiner calls a gateway cannot perform those functions. It must be noted that Chang does not refer to the DLR 50, or to any other device, as a gateway. Presumably then, the Examiner asserts that the DLR 50 is disclosed as performing the functions of a gateway. In order to act as a gateway, a device must pass information between two different networks. Chang simply describes the DLR 50 as "functioning like an HLR." *See* Chang, ¶23. Chang's DLR 50 only provides location information — the DLR never operates as a gateway. The fact that neither the GAN nor the DLR performs the functions of a gateway indicates that the combination of the two components similarly fails to disclose or suggest a

gateway. As a result, it is respectfully asserted that Chang, whether by name or by function, fails to disclose or suggest a gateway connected to a wired network.

In order to bolster the rejection, the Examiner cited U.S. Patent No. 7,356,339 to Nam (hereinafter "Nam"). Preliminarily, it must be recognized that Nam has not been cited as a part of any rejection. It is therefore understood that Nam has been introduced to provide general background information regarding the state of the art. However, the mere fact that Nam describes its GAN as a gateway does not in any way imply that the GAN of Chang should be interpreted as such. As noted above, a GAN is defined simply as a "General ATM switch Network," and such a network in general does not imply the use or the functions of a gateway. The fact that the Examiner has found one reference which describes a GAN as a gateway does not indicate that all GANs include or function as gateways — the network described in Nam is directed toward the particular goals of Nam's invention and has little bearing on Chang (and even less bearing on the present invention). Absent any further description, a GAN is simply a type of switched network, without any sort of gateway functionality implied.

Rebo cannot cure the deficiencies of Chang in this respect. In particular, Rebo is solely concerned with association of a mobile station to wireless access points. Specifically, Rebo teaches a method that provides for authentication between a first wireless access point and neighboring access points, such that, once a mobile station has authenticated itself with the first access point, its authentication context information will be communicated by the first access point to neighboring access points, which allows the station to roam among neighboring access points without requiring new authentication. (See Rebo, Abstract.) However, there is no teaching in Rebo regarding a gateway or its relationship with respect to access points. Thus,

Chang and/or Rebo, taken alone or in combination, fail to disclose or suggest a gateway connected to a wired network.

Claim 1 further recites, "a plurality of access points **associated with, and controlled by, the gateway**" (emphasis added). Since Chang does not disclose or suggest a gateway, Chang cannot disclose or suggest access points associated with or controlled by such a gateway. The same argument applies to Rebo, which similarly fails to disclose or suggest a gateway.

However, assuming *arguendo* that the Examiner's characterization of Chang's GAN is correct, it is nevertheless clear that the cited references do not disclose or suggest access points that are controlled by the "gateway." The Examiner asserts that a combination of GAN 100 and DLR 50 represents the gateway, while access network controllers (ANCs) 20a and 20p represent the access points (e.g., Final Office Action, p.2, ¶3; Advisory Action). However, Chang explicitly states, "The BSM 30 manages the states of the ANCs 20a and 20p in hardware and software…" Chang, ¶23. This base station manager (BSM) is clearly shown as being distinct from both the GAN and the DLR. Thus, contrary to the Examiner's assertion, the states of the ANCs are managed by the BSM 30, and not by the GAN or DLR.

In response, the Examiner first makes assertions about the functionality of the DLR, and second, asserts that the BSM could easily be incorporated into the GAN. Regarding the DLR, the Examiner has argued that "the DLR provides the session information of at terminal to an access node" (Final Office Action, p.4, ¶5). However, upon a closer reading of Chang, it is clear that this provision of session information cannot be reasonably interpreted as "controlling" the access networks. Instead, the access networks request information from the DLR, and the DLR provides only such information as requested. *See* Chang, FIG. 3. As such, the DLR functions

solely as a repository for information and has no control functionality whatsoever. *See* Chang, ¶27.

Regarding incorporation of the BSM into the GAN, and hence, into the Examiner's alleged "gateway", the Examiner asserts generally that such incorporation is known in the art. However, the Examiner has not stated any reason why such a design would be advantageous in the context of Chang so as to render the difference obvious. Instead, the Examiner merely asserts, "There is no reason the BSM … couldn't be integrated into the GAN."

In the first place, it should be noted that the GAN is merely a type of network and is not a "gateway node," as the Examiner asserts, even in the broadest of interpretations. Chang states that the DLR functions may be incorporated into the "packet control function" of the GAN, but the Examiner has not provided any reference which would indicate that BSM functionality could be similarly incorporated. Furthermore, it is not sufficient to state that "there is no reason" a change could not be made. Such reasoning is impermissible hindsight reconstruction analysis. The burden is on the Examiner to state a plausible motivation for incorporating a change in order to render a claim obvious, and this has not been done. *See* MPEP § 2142. The Examiner has not shown that Chang discloses a gateway, that the DLR controls access points, or that the BSM is a part of a gateway. As a result, it is respectfully asserted that Chang fails to disclose or suggest access points which are controlled by a gateway.

Regarding Rebo, as noted above, the reference is solely concerned with authentication and association to wireless access points and there is no teaching of a gateway or its relationship with the access points. Thus, Chang and/or Rebo, taken alone or in combination, fail to disclose or suggest a plurality of access points associated with, and controlled by, a gateway.

Speaking broadly, the remaining elements of claim 1 are tied into interactions with, and configuration of, the gateway. Although the Examiner attempts to tie these elements to Chang's DLR, the fact remains that the DLR does not act as a gateway, whether in combination with the GAN or standing alone. The present specification acknowledges, for instance, that the prior art discloses "a backend authentication server," to deal with session information. *See* present specification, ¶5. However, the present specification also notes that such a solution imposes a high overhead. The present invention addresses these concerns by incorporating some authentication functions into a gateway itself, such that authentication will not be slowed by an authentication server located in a different network segment. *See* present specification, ¶9. Neither Chang nor Rebo is responsive to these concerns, and neither incorporates authentication steps into a gateway. Thus, although there are certain elements of each which seem superficially similar to the present invention, the references are directed toward solving different problems and therefore necessarily arrive at different solutions.

As such, neither Chang nor Rebo, taken singly or in combination, teach the additional above-recited limitations of Claim 1.

Accordingly, Claim 1 is patentably distinct and non-obvious over Chang and Rebo for at least the reasons set forth above. Therefore, withdrawal of the rejection and allowance of Claim 1 is earnestly requested.

C. Whether Claims 4 and 5 are Unpatentable Under 35 U.S.C. §103(a) Over U.S. Patent Publication No. 2004/0203771 to Chang et al. in view of U.S. Patent Publication No. 2008/0119184 to Rebo et al. and further in view of U.S. Patent

Publication No. 2002/0046179 to Kokudo.

Claims 4 and 5 are rejected as being unpatentable over U.S. Patent Publication No. 2004/0203771 to Chang et al. (hereinafter "Chang") in view of U.S. Patent Publication No. 2008/0119184 to Rebo et al. (hereinafter "Rebo") and further in view of U.S. Patent Publication No. 2002/0046179 to Kokudo (hereinafter "Kokudo"). The Examiner contends that the cited combination shows all the limitations recited in Claims 4 and 5. Appellants respectfully disagree.

Chang is directed to a method of managing information about mobile terminal in a mobile communication system supporting high-rate data transmission, and further discloses:

> "A method of managing the session information of an AT in a CDMA2000 IxEV-DO system. In the IxEV-DO system, a service system, having an SC/MM, is connected to a PDSN, a plurality of ANs are connected to the service system, and a plurality of ATs are capable of wireless communication with the ANs. In the session information managing method, an AN transmits to the SC/MM a session retrieve request message, upon receipt of a connection request message from the AT. The SC/MM then searches for session information of the AT and transmits to the AN a session retrieve response message including the session information. Upon receipt of the session retrieve response message, the AN transmits a connection response message to the AT." (Chang, Abstract)

Rebo is directed to a method for fast, secure 802.11 re-association without additional authentication, accounting, and authorization infrastructure, and further discloses:

> "A method wherein an access point authenticates itself with neighboring access points and establishes secure and mutually authenticated communication channels with its neighboring access points. When an access point learns of a neighboring access point, it initiates an authentication with an authentication server through the neighboring access point. Once access points have mutually authenticated each other, whenever a station authenticates itself with a first access point, the first access point communicates the station's authentication context information, for example session key and session identifier, to each neighboring access point. Thus, when the station roams to a neighboring access point, the neighboring access point presents the station with a reauthentication protocol, for example LEAP reauthentication, and

> if the reauthentication is successful, communication between the station and the neighboring access point takes place immediately and no new EAP authentication needs to occur." (Rebo, Abstract)

Kokudo is directed to a "virtual public access service" (Kokudo, Title). In further detail, Kokudo discloses the following in the Abstract:

> "A method for offering a virtual public access service is provided, which makes it easier for mobile users to have access to a network (e.g., the Internet and/or LAN) by radio, and which makes it possible to realize faster communication than the existing public mobile telephone network. In the step (a), a contract is made by a provider of a virtual public access service, with a network owner/manager who owns and/or manages a network system that are accessible to authorized network users. The contract includes a clause that the network owner/manager gives the provider permission to place a radio access point device that forms a radio access point in the network system and to connect the radio access point to the Internet by way of the network system. The contract further includes a clause that the network owner/ manager can get payment for the permission from the provider. In the step (b), a radio access point device that forms a radio access point is placed by the provider in the network system of the network owner/manager in accordance with the contract, thereby forming a virtual public network. The virtual public network allows registered users of the provider to access the Internet by way of the radio access point and the network system."

It will be shown below that the limitations of Claims 4 and 5 reproduced herein (as argued separately and with respect to independent Claim 1 from which they depend) are not shown in the cited combination, and that Claims 4 and 5 should be allowed.

C1. Claims 4 and 5

Initially, it is respectfully pointed out to the Examiner that Claims 4 and 5 directly or indirectly depend from independent Claim 1. Thus, Claims 4 and 5 include all the limitations of Claim 1.

As previously discussed in connection with Claim 1, neither Chang nor Rebo teaches or suggests at least the features of "a gateway connected to a wired network; and a plurality of access points associated with, and controlled by, the gateway." These features are provided in Claims 4 and 5 by virtue of their respective dependency (directly or indirectly) from Claim 1.

Furthermore, there is no teaching in Kokudo of any control relationship between gateway 14 and access point device 8. Thus, Appellants submit that Chang, Rebo and/or Kokudo, either singly or in combination, fail to disclose or suggest a gateway or access points controlled by the gateway, as provided in Claims 4 and 5.

Claims 4 and 5 (with the following applicable to Claim 5 by virtue of its dependency from Claim 4) further recite, *inter alia*, "means to ensure that a connection between the gateway and an access point is trusted." The Examiner concedes that Chang and Rebo fail to disclose this element, but asserts that Kokuda does disclose it.

The Examiner asserts that "encrypted gateway," as disclosed by Kokuda in paragraph 32, "implies communications between access point and gateway are encrypted." However, this is demonstrably false. Kokuda shows that encryption is used to secure communications between the gateway 14 and the ISP network 6, not between the gateway 14 and the access point 8. *See* Kokuda, ¶97 and FIG. 2, block 15. In fact, the access point 8 and gateway 14 of Kokuda are disclosed as being part of the same apparatus. *See* Kokuda, ¶94. Thus there is no need for encryption between the two, and the addition of such would be wholly superfluous. As a result, it is respectfully asserted that Chang, Rebo, and/or Kokuda, taken alone or in any combination, fail to disclose or even remotely suggest a trusted connection between a gateway and an access point.

As such, neither Chang, Rebo, nor Kokuda, taken singly or in combination, teaches or suggests the above-recited limitations of Claims 4 and 5.

Accordingly, Claims 4 and 5 are patentably distinct and non-obvious over Chang, Rebo, and/or Kokudo for at least the reasons set forth above. Therefore, withdrawal of the rejection and allowance of Claims 4 and 5 is earnestly requested.

D. Conclusion

For reasons set forth above, Appellants submit that all of the pending claims are not obvious in view of the teachings of the cited references. Accordingly, it is respectfully requested that the rejections of Claims 1, 4 and 5 under 35 U.S.C. §103(a) be reversed.

Respectfully submitted,

September 9, 2009
Date

/Wan Yee Cheung/
Wan Yee Cheung
Attorney for Appellants
Registration No.: 42,410
Telephone No.: 609-734-6834

Thomson Licensing LLC
Patent Operations
P.O. Box 5312
Princeton, NJ 08543-5312

8. Claims Appendix

1. (Previously presented) A communications system, comprising:

a gateway connected to a wired network; and

a plurality of access points associated with, and controlled by, the gateway,

wherein each access point is configured (i) to wirelessly communicate with and receive association requests from wireless clients for connection to the wired network through the access point (ii) to send session information requests to the gateway in response to received association requests and (iii) to process session information setting commands received from the gateway,

wherein the gateway is configured (i) to maintain session information that currently exists for each wireless client connected to the wired network through an access point associated with the gateway, the session information including a session key associated with each wireless client and an associated access point, and (ii) to respond to a session information request from a given access point by providing that access point with currently existing session information, if any, maintained by the gateway for the wireless client requesting association with that access point.

2. (Previously presented) The system of claim 1 wherein each access point is configured to maintain a session key per associated wireless client.

3. (Previously presented) The system of claim 1 wherein each access point is configured to remove session information after a wireless client becomes disassociated with that access point by either responding to a command sent to the access point from the gateway to remove the

session information or automatically removing idle wireless client session information entries after a predetermined period of inactivity.

4. (Original) The system of claim 1 having means to ensure that a connection between the gateway and an access point is trusted.

5. (Original) The system of claim 4 wherein the means comprises physical security or encryption.

6. (Previously presented) A method of enabling roaming of wireless clients among wireless access points in a network comprising the steps of (a) providing a gateway in the network in control of the wireless access points, sending session data requests from access points to the gateway, the session data including a session key associated with each wireless client and an associated access point, (b) looking up session data stored in the gateway, reporting session data failure if session data is not found, and (c) sending a session data response from the gateway to the access point if session data is found or is generated by the gateway;

wherein an association request from a wireless client is received by an access point and, after receiving a session data failure response from the gateway, the access point generates session data, reports the generated session data to the gateway and sends an association response to the wireless client.

7. (Original) The method of claim 6 wherein an association request from a wireless station is received by an access point and, after receiving a session data response from the gateway, the access point loads session data and sends the session data to the wireless client.

8. (Cancelled)

9. (Previously presented) The method of claim 6 comprising removing session information from the previously associated access point after a wireless client becomes associated with a new access point comprising the gateway sending a command to the previously associated access point to remove the session information or automatically removing idle wireless client entries after a predetermined period of inactivity.

10. (Original) The method of claim 6 wherein the gateway authenticates an access point to ensure that a connection between the gateway and the access point is trusted.

11. (Original) The method of claim 10 wherein the authentication is encrypted.

12. (Cancelled)

13. (Previously presented) A computer readable medium encoded with instructions that are executable by a processor in a wireless access point in a network for the wireless access point device to perform the steps of:

receiving an association request from a wireless client;

communicating with a gateway connected to the network to obtain currently existing session information maintained by the gateway, if any, which is associated with the wireless client requesting association to the wireless access point, the session information comprising a session key associated with the wireless client and an associated wireless access point;

receiving a session data response from the gateway, which includes currently existing session information for the wireless client requesting association to the wireless access point; and

loading the session information into the wireless access point and sending the session information to the wireless client in an association response transmitted to the wireless client.

14. (Previously presented) The computer readable medium of claim 13, further encoded with instructions executable by the processor for the wireless access point to perform steps of:

receiving a session data failure response from the gateway indicating that no session information currently exists for the wireless client, and

in response to said received data failure response, generating session data, reporting the generated session data to the gateway and sending an association response to the wireless client.

15. (Previously presented) The computer readable medium of claim 13, further encoded with instructions executable by the processor for the wireless access point to perform a step of removing session information for a wireless client previously associated with the wireless access point after the wireless client becomes associated with a new wireless access point.

16. (Previously presented) The computer readable medium of claim 13, further encoded with instructions that are executable by the processor of the wireless access point device to perform an authentication process to ensure that a connection between the gateway and the wireless access point is trusted.

17. (Previously presented) The computer readable medium of claim 16 wherein the authentication comprises encrypted communications with the gateway.

18. (Previously presented) The computer readable medium of claim 15, wherein removing session information for the wireless client is performed by the wireless access point in response to a command sent by the gateway to remove that session information.

19. (Previously presented) The computer readable medium of claim 15, wherein removing session information for a wireless client is performed automatically by the wireless access point removing idle wireless client session information entries for the wireless client after a predetermined period of inactivity of the wireless client.

9. Related Evidence Appendix

None.

10. Related Proceedings Appendix

None